Nicholas A. Carlin, State Bar No. 112532
David M. Given, State Bar No. 142375
PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
The Presidio
San Francisco, CA 94129
Tel: (415) 398-0900
Fax: (415) 398-0911
Email: nac@phillaw.com

Attorneys for Plaintiff DAN ALEXANDER

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DAN ALEXANDER. on behalf of himself and all others similarly situated,

Plaintiff,

v.

EQUIFAX INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

SUMMARY OF THE CASE

1. On September 7, 2017, Equifax Inc. announced that hackers had breached a Web-based application for Equifax and obtained sensitive personal information of approximately 143 million American consumers. The personal information obtained in the breach included social security numbers, birth dates and home addresses. Equifax also said it lost control of an unspecified number of driver's license numbers, along with the credit card numbers of 209,000 consumers and credit dispute documents for 182,000 consumers. The breach began in May, 2017 and was discovered in July, 2017.

2. Equifax is one of the three largest U.S. based credit reporting agencies that collect and analyze detailed financial records for consumers worldwide

3. Plaintiff Dan Alexander brings this lawsuit against Equifax individually and on behalf of a nationwide class including all other similarly situated consumers of Equifax.

PARTIES

4. Plaintiff Dan Alexander is a resident of Los Angeles, California.

5. On information and belief, defendant Equifax, Inc. is a Georgia corporation with its headquarters located in Atlanta, Georgia. The company is a consumer credit reporting agency that gathers and maintains information on over 800 million consumers and 88 million businesses. Founded in 1899 as Retail Credit Company, the company is the oldest of the three largest American credit agencies. Equifax is a multi-billion dollar company and is one of 55 contractors hired by the United States Department of Health and Human Services to work on the Healthcare.gov website.

JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (a) at least one member of the putative class is a citizen of a state different from Equifax, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none of the exceptions under the subsection apply to this action.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

7. This Court has jurisdiction over Defendant because it is registered to conduct business in California, has sufficient minimum contacts in California, or otherwise intentionally avails itself of the markets within California, through the promotion, sale, marketing and distribution of their products in California, to render the exercise of jurisdiction by this Court proper and necessary.

8. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant conducts substantial business in this District.

COMMON FACTUAL ALLEGATIONS

9. On September 7, 2017, Equifax Inc. announced that hackers had breached a Web-based application for Equifax and obtained sensitive personal information of approximately 143 million American consumers. The personal information obtained in the breach included social security numbers, birth dates and home addresses. Equifax also said it lost control of an unspecified number of driver's license numbers, along with the credit card numbers of 209,000 consumers and credit dispute documents for 182,000 consumers. The breach began in May, 2017 and was discovered in July, 2017, but Equifax did not notify the public until September 7, 2017.

Equifax's Security Practices are Inadequate

10. Despite growing efforts by hackers to access personal information maintained by credit service companies and the emphasis on data security in the credit service industry, Equifax (1) failed to implement security measures and technological safeguards designed to prevent this type of attack even though the credit services industry has been repeatedly warned about the risk of cyberattacks, (2) failed to employ security protocols to detect the unauthorized network activity, and (3) failed to maintain basic security measures.

Over 143 Million American Consumers are Victims of the Breach

11. As a result of Equifax's negligent security practices and the delay in notifying affected consumers, these consumers are subject to an increased and real risk of identity theft based on the breach of their personal information by Equifax.

12. Affected consumers will have to spend time and money securing their personal information and protecting their identities. They will need to monitor their accounts and credit,

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

and will have to pay for further credit monitoring services in the wake of the data breach to make sure their identities were not harmed by anyone who may have stolen their information.

13. The disclosure of Social Security numbers in particular poses significant risks. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Former and current Equifax consumers whose Social Security numbers have been compromised have spent time contacting various agencies, such as the Internal Revenue Service, the Social Security Administration, and their local state tax boards. They also now face a real and immediate risk of identity theft and other problems associated with the disclosure of their Social Security number, and will need to monitor their credit and tax filings for an indefinite duration. Individuals cannot even obtain a new Social Security number until there is evidence of ongoing problems due to misuse of the Social Security number.

PLAINTIFF'S EXPERIENCE

14. At relevant times hereto, Equifax collected and stored personal and credit information from Plaintiff, including his social security number, birth date, home address, driver's license information and credit card numbers.

15. On September 8, 2017, after hearing of the data breach, Plaintiff went to the "Check Potential Impact" web site set up by Defendant to determine if his information had been compromised. The response was: "Based on the information provided, we believe that your personal information may have been impacted by this incident." Accordingly, Plaintiff is informed and believes that his information has been compromised.

CLASS ACTION ALLEGATIONS

16. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and the following classes:

> All California consumers whose personal or credit data was stored by Equifax, whose data was accessed by the hackers or who were subject to risk of their data being accessed by hackers from January 1, 2016 to the present (the "California Class").

All Nationwide consumers in the United States whose personal or credit data was stored by Equifax, whose data was accessed by the hackers or who were subject to risk of their data being accessed by hackers from January 1, 2016 to the present (the "Nationwide Class").

Excluded from the proposed classes are anyone employed by counsel for Plaintiff in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

17. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

18. Numerosity. The proposed classes consist of over 143 million American consumers who had their data stolen in the Equifax data breach, making joinder of each individual class member impracticable.

19. Commonality. Common questions of law and fact exist for the proposed classes' claims and predominate over questions affecting only individual class members.

Common questions include:

a. Whether Equifax violated California Civil Code sections 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether Equifax violated California Civil Code section 1798.82 by failing to promptly notify class members that their personal information had been compromised;

c. Whether Equifax acted negligently in failing to maintain adequate security procedures and practices;

d. Whether Equifax breached its contractual promises to adequately protect class members' personal information;

e. Whether Equifax's failure to implement adequate security constitutes an unfair, unlawful, or deceptive practice under state consumer protection law;

f. Whether class members may obtain damages, restitution, declaratory, and injunctive relief against Equifax; and

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

g. What security procedures and data-breach notification procedure Equifax should be required to implement as part of any injunctive relief ordered by the Court.

20. Typicality. Plaintiff's claims are typical of the claims of the proposed classes because, among other things, Plaintiff and class members sustained similar injuries as a result of Equifax's uniform wrongful conduct and their legal claims all arise from the same core Equifax's practices.

21. Adequacy. Plaintiff will fairly and adequately protect the interests of the classes. His interests do not conflict with class members' interests and he has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the classes.

22. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Equifax's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

23. In addition, class certification is appropriate under Rule 23(b)(1) or (b)(2) because:

a. the prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Equifax;

b. the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

c. Equifax has acted or refused to act on grounds that apply generally to the proposed classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole.

FIRST CAUSE OF ACTION

For Violation of the California Customer Records Act,

California Civil Code Section 1798.80, *et seq.*

24. Plaintiff incorporates the above allegations by reference.

25. Plaintiff brings this cause of action on behalf of the California Class whose personal information is maintained by Equifax and/or that was compromised in the data breach announced in September 2017.

26. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted California Customer Records Act. This statute states that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Civil Code section 1798.81.5.

27. Equifax is a "business" within the meaning of Civil Code section 1798.80(a).

28. Plaintiff and members of the class are "individual[s]" within the meaning of the Civil Code section 1798.80(d). Pursuant to Civil Code sections 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes an individual's name, Social Security number, driver's license or state identification card number, and debit card and credit card information. "Personal information" under Civil Code section 1798.80(e) also includes address, telephone number, passport number, education, employment, or employment history.

29. The breach of the personal data of over one hundred millions of Equifax consumers instituted a "breach of the security system" of Equifax pursuant to Civil Code section 1798.82(g).

30. By failing to implement reasonable measures to protect its consumers' personal data, Equifax violated Civil Code section 1798.81.5.

31. In addition, by failing to promptly notify all affected consumers that their personal information had been acquired (or was reasonably believed to have been acquired) by

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

unauthorized persons in the data breach, Equifax violated Civil Code section 1798.82 of the same title. Equifax's failure to timely notify consumers of the breach has caused damage to class members who have had to buy identity protection services or take other measures to remediate the breach caused by Equifax's negligence.

32. By violating Civil Code sections 1798.81.5 and 1798.82, Equifax "may be enjoined" under Civil Code section 1798.84(e).

33. Accordingly, Plaintiff requests that the Court enter an injunction requiring Equifax to implement and maintain reasonable security procedures to protect customers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Equifax, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) ordering that Equifax engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Equifax, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (7) ordering Equifax to encrypt sensitive personal information.

34. Plaintiff further requests that the Court require Equifax to (1) identify and notify all members of the class who have not yet been informed of the data breach; and (2) to notify affected former and current consumers of any future data breaches by email within 24 hours of Equifax's discovery of a breach or possible breach and by mail within 72 hours.

35. As a result of Equifax's violation of Civil Code sections 1798.81.5, and 1798.82, Plaintiff and members of the class have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

36. Plaintiff, individually and on behalf of the members of the California Class, seeks all remedies available under Civil Code section 1798.84, including, but not limited to: (a) damages suffered by members of the class; and (b) equitable relief.

37. Plaintiff, individually and on behalf of the members of the California Class, also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

SECOND CAUSE OF ACTION

For Unlawful and Unfair Business Practices Under

California Business and Professions Code § 17200, *et seq.*

38. Plaintiff incorporates the above allegations by reference.

39. Plaintiff brings this cause of action on behalf of the California class whose personal information was compromised as a result of the data breach publicized in September 2017.

40. Equifax's acts and practices, as alleged in this complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.

41. The acts, omissions, and conduct of Equifax also constitute a violation of the unlawful prong of the UCL because it failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977 and California Customer Records Act, which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

42. In failing to protect consumers' personal information and unduly delaying informing them of the data breach, Equifax has engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and the Information Practices Act of 1977. In enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). Equifax's conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, et seq., which seeks to protect individuals' data

and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

43. As a direct and proximate result of Equifax's unlawful and unfair business practices as alleged herein, Plaintiff and members of the class have suffered injury in fact. Plaintiff and the class have been injured in that their personal information has been compromised and they are at an increased risk for future identity theft and fraudulent activity on their financial accounts. Class members have also lost money and property by purchasing credit monitoring services they would not otherwise had to but for Equifax's unlawful and unfair conduct.

44. As a direct and proximate result of Equifax's unlawful and unfair business practices as alleged herein, Plaintiff and class members face an increased risk of identity theft and medical fraud, based on the theft and disclosure of their personal information.

45. Because of Equifax's unfair and unlawful business practices, Plaintiff and the class are entitled to relief, including restitution to Plaintiff and class members for costs incurred associated with the data breach and disgorgement of all profits accruing to Equifax because of its unlawful and unfair business practices, declaratory relief, and a permanent injunction enjoining Equifax from its unlawful and unfair practices.

46. The injunctive relief that Plaintiff and members of the class are entitled to includes, but is not limited to: (1) ordering that Equifax, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) ordering that Equifax engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Equifax, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (6) ordering Equifax to meaningfully educate its former and current consumers about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (7) ordering Equifax to

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

encrypt sensitive personal information.

47. Plaintiff, individually and on behalf of the members of the class, also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

THIRD CAUSE OF ACTION

Negligence

48. Plaintiff incorporates the above allegations by reference.

49. Plaintiff brings this cause of action on behalf of the Nationwide Class whose personal information was compromised as a result of the data breach publicized in September 2017.

50. In collecting the personal information consumers, Equifax owed Plaintiff and members of the class a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing Equifax's security systems and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiff and the class from unauthorized access and use. Equifax's security system and procedures for handling the personal information of consumers were intended to affect Plaintiff and the class. Equifax was aware that by taking such sensitive information of consumers, it had a responsibility to take reasonable security measures to protect the data from being stolen and, in the event of theft, easily accessed.

51. The duty Equifax owed to Plaintiff and members of the class to protect their personal information is also underscored by the California Customer Records Act and

52. Additionally, Equifax had a duty to timely disclose to Plaintiff and members of the class that their personal information had been or was reasonably believed to have been compromised. Timely disclosure is appropriate so that Plaintiff and members of the class could, among other things, report the theft of their Social Security numbers to the Internal Revenue Service, monitor their credit reports for identity fraud, undertake appropriate measures to avoid unauthorized charges on their debit card or credit card accounts, and change or cancel their debit or credit card PINs (personal identification numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized transactions.

53. There is a very close connection between Equifax's failure to take reasonable security standards to protect its consumers' data and the injury to Plaintiff and the class. When individuals have their personal information stolen, they are at risk for identity theft, and need to

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

buy credit monitoring services and purchase credit reports to protect themselves from identity theft.

54. Equifax is morally to blame for not protecting the data of its consumers by failing to take reasonable security measures. If Equifax had taken reasonable security measures, data thieves would not have been able to take the personal information of over 143 million American consumers.

55. The policy of preventing future harm weighs in favor of finding a special relationship between Equifax and the class. Equifax's consumers count on Equifax to keep their data safe and in fact are required to share sensitive personal data with Equifax as a condition Equifax's services. If companies are not held accountable for failing to take reasonable security measures to protect their customers' personal information, they will not take the steps that are necessary to protect against future data breaches.

56. It was foreseeable that if Equifax did not take reasonable security measures, the data of Plaintiff and members of the class would be stolen. Major corporations, particularly those in the credit services industry, like Equifax, face a higher threat of security breaches than other companies due in part to the large amounts and type of data they possess. Equifax should have known to take precautions to secure its consumers' data, especially in light of recent data breaches and warnings regarding cyberattacks and network vulnerability in the credit services industry.

57. Equifax breached its duty to exercise reasonable care in protecting the personal information of Plaintiff and the class by failing to implement and maintain adequate security measures to safeguard its consumers' personal information, failing to monitor its systems to identify suspicious activity, allowing unauthorized access to the personal information of Plaintiff and the class, and failing to encrypt or otherwise prevent unauthorized reading of such personal information.

58. Equifax breached its duty to timely notify Plaintiff and the class about the data breach. Additionally, Equifax was, or should have been, aware of breaches in its network security as early as May of 2017.

59. But for Equifax's failure to implement and maintain adequate security measures to protect its consumers' personal information and failure to monitor its systems to identify

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900

suspicious activity, the personal information of Plaintiff and members of the class would not have been stolen, and they would not be at a heightened risk of identity theft in the future.

60. Equifax's negligence was a substantial factor in causing harm to Plaintiff and members of the class.

61. As a direct and proximate result of Equifax's failure to exercise reasonable care and use commercially reasonable security measures, the personal information of current and former Equifax consumers was accessed by unauthorized individuals who could use the information to commit identity fraud, medical fraud, or debit and credit card fraud. Plaintiff and the class face a heightened risk of identity theft in the future.

62. Members of the class have also suffered economic damages, including the purchase of credit monitoring services they would not have otherwise purchased.

63. Neither Plaintiff nor other members of the class contributed to the security breach, nor did they contribute to Equifax's employment of insufficient security measures to safeguard personal information.

64. Plaintiff and the class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed classes, requests that the Court:

a. Certify this case as a class action on behalf of the classes defined above, appoint Dan Alexander as class representative, and appoint Phillips, Erlewine, Given & Carlin LLP and Nicholas A. Carlin as class counsel;

b. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other class members;

c. Award restitution and damages to Plaintiff and class members in an amount to be determined at trial but at least $5,000,000;

d. Award Plaintiff and class members their reasonable litigation expenses and attorneys' fees;

e. Award Plaintiff and class members pre- and post-judgment interest, to the extent allowable; and

f. Award such other and further relief as equity and justice may require.

Date: September 8, 2017

Respectfully Submitted,

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP

By: */s/ Nicholas A. Carlin*

Nicholas A. Carlin

JURY DEMAND

Plaintiff hereby demands a jury trial on all issues so triable.

Date: September 8, 2017

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP

By: */s/ Nicholas A. Carlin*

Nicholas A. Carlin

ATTESTATION

I, Nicholas A. Carlin, am the ECF user whose identification and password is being used to file the instant document. I hereby attest that all counsel whose electronic signatures appear above provided their authority and concurrence to file this document.

/s/ Nicholas A. Carlin

Nicholas A. Carlin

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
San Francisco, CA 94129
(415) 398-0900